

## **SECURITY FOR UNIQUELY GENERATED ELECTRONIC SEALS OF CERTIFICATION**

5 This application is a continuation patent application and claims priority from co-  
pending U.S. Patent Application Serial No. 09/634,149, filed August 8, 2000, the entire  
content of which is incorporated herein by reference.

### **TECHNICAL FIELD**

The present invention relates to electronic seals.

10

### **BACKGROUND**

One of the difficulties a user faces when engaging other parties online, such as  
joining online clubs, purchasing items or generally interacting with others, is that the  
user typically has limited contact with the other parties and, therefore, often has privacy  
concerns and other legitimate apprehensions. This is especially true when the user  
15 wishes to conduct business online, such as in an online marketplace or business-to-  
business intermediary. As a result, some organizations have established “seal  
programs” by setting policies and issuing electronic “seals” to companies that adhere to  
the policies. For example, TRUSTe™ is an independent, non-profit privacy  
organization that has developed a third-party oversight seal program that tries to  
20 alleviate users' concerns about online privacy, TRUSTe issues an electronic seal image  
to organizations that meet its privacy program. The certified organizations display the  
seal on their websites to indicate their compliance with the program.

### **SUMMARY OF THE INVENTION**

25 In general, the invention provides techniques for issuing electronic seals such  
that non-certified parties cannot easily steal or otherwise misuse the seals. According to  
one aspect of the invention, a central seal “issuer” verifies the credentials, policies or  
business practices of online merchants and issues a corresponding seal of certification  
upon verification. Unlike conventional systems, the seal issuer can generate a unique  
seal for each merchant. The seal issuer generates the seal in the form of a media object

that includes an encrypted watermark containing an expiration date. A central seal server stores the media objects such that the merchants can dynamically retrieve and display the electronic seals as needed. The seal issuer, therefore, can easily revoke or update the seals on the central seal server.

5           In another aspect, the invention is directed to a method in which a database is accessed to retrieve certification data for a set of online merchants and a corresponding media object is generated for each merchant as a function of the certification data. Each media object represents a seal of certification for the corresponding online merchant. In one configuration, the media objects are generated by an embedding an encrypted  
10       digital watermark having an expiration date for the seal. The media objects are stored on a seal server such that each media object can be retrieved according to a unique identifier for the corresponding merchant. Upon receiving such a request, the requested media object is communicated to a client device for presentment to a user.

          In yet another aspect, the invention is directed to a computer-readable medium  
15       having instructions configured to cause a programmable-processor to perform the methods described herein.

          The invention offers several advantages over conventional systems. For example, because the media objects are centrally stored by the seal issuer, and can be unique to each online merchant, each seal can easily be revoked or updated.  
20       Furthermore, requests to display the seals can more easily be tracked such that general usage can be reported and misuse can be detected.

          Various embodiments of the invention are set forth in the accompanying drawings and the description below. Other features and advantages of the invention will become apparent from the description, the drawings, and the claims.

## 25                               **BRIEF DESCRIPTION OF THE DRAWINGS**

          Figure 1 is a high-level block diagram of an example system configured according the invention.

          Figure 2 is a more detailed block diagram of an example system configured according to the invention.

Figure 3 is a flowchart illustrating an example process in which the system certifies online merchants.

Figure 4 is a flowchart illustrating an example process in which the system generates and maintains a set of media objects that represent electronic seals of certification.

Figure 5 is a flowchart illustrating an example process in which the system services requests from the online merchants to present the electronic seals.

Figure 6 is a flowchart illustrating an example process in which the system services requests from users to view certification information for the online merchants.

10

## DETAILED DESCRIPTION

Figure 1 is a high-level block diagram of a system 2 in which online merchants 4 provide goods and services to user 6. Merchants 4 represent business entities that transact goods or services over network 12, which represents a network of computing resources such as the Internet. For example, a merchant 4 can be a buyer or seller of goods, such as books, movies, software, computers, semiconductor components and the like. A merchant 4 can also be an entity that provides services over network 12, such as an online storage provider, an Application Service Provider (ASP) or even an online marketplace or other intermediary. Although described in the context of a business entity, merchants 4 can also be any entity having an online presence.

User 6 uses computing device 10 to remotely interact with merchants 4 over network 12. Computing device 10 represents any communication device suitable for interfacing with network 12 and interacting with merchants 4 such as a personal computer running a web browser such as Internet Explorer™ from Microsoft Corporation of Redmond, Washington. Alternatively, computing device 4 can be, for example, a personal digital assistant (PDA), such as a Palm™ organizer from Palm Inc. of Santa Clara, California, or a network-enabled cellular telephone.

Seal issuer 8 verifies the credentials, policies or business practices of each Merchant 4 and issues a corresponding seal of certification to each merchant 4 upon verification. In order to become a “seal holder”, each merchant 4 must comply with requirements set by seal issuer 8. For example, seal issuer might, for example, verify

that merchant 4 is a legitimate business merchant that complies with, or agrees to conform to, certain standards. For example, seal issuer 8 may be an online dispute resolution service that is designed to help buyers and sellers settle issues involving online transactions, such as issues that may arise in an online auction. In this instance, seal issuer 8 issues an electronic seal to merchants 4 that agree to participate in the web-based problem solving service. As another example, seal issuer 8 can be an organization that verifies merchants 4 compliance with privacy or security requirements. Alternatively, for example, seal issuer 8 may perform a nominal amount of certification before issuing the seal such as verifying the contact information.

Upon verifying a merchant 4, seal issuer 8 issues the merchant 4 an electronic seal that is a recognizable symbol associated with certain qualities such as trustworthiness, reliability, and superior customer service. Merchants 4 post their corresponding electronic seals on their web sites or in electronic mail messages (emails) in order to increase the confidence of potential customers. Unlike conventional techniques, seal issuer 8 does not issue a static image to merchants 4. As described in detail below, seal issuer 8 generates and maintains a unique electronic seal for each merchant 4. As such, seal issuer 8 can instantly issue, update, change, or revoke a seal when a merchant 4 fails to comply with the requirements. In addition, seal issuer 8 tracks the use of all issued electronic seals in order to detect any misuse or theft of the seal.

Figure 2 is a block diagram illustrating one example of seal issuer 8. Seal issuer 8 includes web servers 20, seal servers 22, administration (“admin”) server 26, database 23, request log 24 and seal repository 25.

Web servers 20 provide an interface for communicating with computing device 10 via network 12. Web servers 20 execute web server software, such as Internet Information Server™ from Microsoft Corporation, of Redmond, Washington, and provide an environment for interacting with users 6 and merchants 4, such as when merchants 4 apply for seals or when users 6 request more information about a certified merchant 4. Web servers 20 serve web pages and communicate the web pages over network 12. The web pages may include static media such as text and graphic imagery,

as well as conventional input media such as text entry boxes, radio buttons, drop-down menus, and the like.

Seal servers 22 provide access to seal repository 25, which stores a set of media objects that represent the electronic seals. Each media object contains media, such as  
5 image data, video data, and audio data, that merchant 4 presents as an electronic seal of certification. Each media object corresponds to one of the merchants 4 and can be retrieved from seal repository 25 based on a unique identifier for the corresponding merchant. In one configuration, each media object is given a unique file name and stored within a file system provided by seal server 22 such that computing device 10  
10 can directly retrieve the media object without requiring that seal issuer 8 access a database. In addition to the media, such as the image data, each media object contains a watermark having encrypted information such as an expiration date, a time stamp and the unique identifier for the corresponding merchant 4.

Database 23 stores information for each merchant 4 such as current certification  
15 status, contact information and an expiration date for each merchant's unique seal. Request log 24 stores all requests for the media objects and the merchant information.

Admin server 26 provides administrative functionality for seal issuer 8 and provides an operating environment for a number of software modules including seal maintenance modules 27 and theft detection modules 28. Seal maintenance modules 27  
20 are responsible for generating a unique media object when a new merchant 4 is certified and updating the media object if the merchant loses its certified status. In addition, seal maintenance modules 27 periodically regenerate the media objects, including updating the embedded expiration date and the timestamp.

Upon certifying a merchant 4, seal maintenance modules 27 generate a  
25 corresponding media object and issue code for use by the merchant to uniquely reference the media object. For example, a merchant 4 having a unique identifier of 1520511267 can use the following code to reference a media object housed within seal servers 22:

30       <a HREF="http://sealissuer.com/1520511267.map"  
          TARGET="\_blank"><IMG ISMAP SRC="http://

```
sealissuer.com/1520511267.gif" ALT="Click to verify"  
BORDER=0></a>
```

5 The above code uses server-side image maps such that when user 6 clicks on any area of the presented image, the pixel coordinate information is transmitted to seal issuer 8 where it is remotely translated into an appropriate action. This advantageously removes any client-side scripting dependencies and greatly reduces the size of the client-side code required to display the seal.

10 Theft detection modules 28 analyze request log 24 in order to detect any misuse or theft of an electronic seal. For example, when a seal is requested, seal servers 22 record the internet protocol (IP) address of the requesting merchant within request log 24. In addition, when user 6 clicks on the seal to verify the seal, web servers 20, provide the information to the user and log the IP address of computing device 10. Theft detection modules 28 analyze request log 24 to detect any new or unexpected IP  
15 addresses. Upon detecting misuse, seal maintenance modules 27 issue a new seal to the affected merchant 4 by generating a new media object, storing the media object within seal repository 25, and instructing the merchant to update its website software to point to the new seal.

20 Theft detection modules 28 also use spidering technology to search network 12 for all occurrences of issued seals. Upon finding a seal, theft detection modules 28 decrypt the embedded watermark, determine whether the seal has expired, inform any interested parties of the expiration and optionally revoke the expired seal.

Figure 3 is a flowchart illustrating an example process 30 in which seal issuer 8 certifies an online merchant 4. First, seal issuer 8 receives an application from  
25 merchant 4 including contact information, business organization and location. This request may be received electronically via network 12 or through conventional communication mechanisms such as the postal service (step 32). Seal issuer 8 researches merchant 4, verifies that the merchant is a legitimate business organization and certifies that the merchant's business practices meet all standards necessary to  
30 obtain the seal (step 34). Upon certifying merchant 4, seal issuer 8 stores the certification data in database 23 (step 36).

Figure 4 is a flowchart illustrating an example process 40 in which seal issuer 8 generates and maintains the media objects within seal repository 25. Upon verifying one or more merchants 4, seal maintenance modules 27 access database 23 and retrieve the certification data for each certified merchant 4. Next, based on this information, seal maintenance modules 27 generate a unique media object for each merchant 4 (step 44) and store the media objects within seal servers 22 (step 46) such that computing device 10 can remotely access the media objects. Next, seal maintenance modules 27 periodically regenerate the media objects in order to update the embedded information including the expiration date (step 48). For example, a new set of media objects can be generated daily in order to facilitate detection of expired seals. In one configuration, seal issuer 8 generates a media object having a transparent image when the corresponding merchant 4 loses its certification status. In this manner, the seal “disappears” from the merchant web site.

Figure 5 is a flowchart illustrating an example process 50 in which seal issuer 8 services requests from the online merchants 4 to present the electronic seals to user 6. When user 6 accesses a merchant 4, client device 10 is directed to retrieve a seal from seal servers 22. More specifically, seal servers 22 receive a request from computing device 10 that includes a unique identifier for one of the merchants and, therefore, uniquely identifies one of the media objects within seal repository 25 (step 52). Seal servers 22 log the request by storing the IP address within request log 24 (step 54) and select the appropriate media object according to the unique identifier (step 56). For example, seal servers 22 may simply identify an appropriate file that stores the media object based on the unique identifier. Upon selecting the media object, seal servers 22 communicate the media object to computing device 10, which in turn presents the media to user 6 (step 58).

Figure 6 is a flowchart illustrating an example process 60 in which the seal issuer 8 services user requests to verify a seal by viewing certification information for the online merchants 4. After the media is presented to user 6, as described above, the user 6 has the option to click on the displayed media to view the certification information for the merchant 4. For example, when the user clicks an image, web servers 20 receive pixel information describing where the user clicked on the image as

well as a unique identifier for the merchant (step 62). Upon receiving the request, web servers 20 log the request (step 64) and access database 23 to retrieve information relating to the identified merchant (step 66). Web servers 20 assemble the retrieved data into a web page and serve the web page to client device 10 for display to user 6 (step 68). Alternatively, web servers 20 direct computer device 10 to a static web page for the corresponding merchant 4.

In one configuration, web servers 20 filters the information based on one or more stored settings, such as an anonymity parameter, which causes web servers 20 to filter contact information for the merchant 4. In another configuration, web servers 20 monitor the requesting universal resource locator (URL) for merchant 4 and filter the information accordingly. In this manner, seal issuer 4 can filter contact information when the seal is used by online intermediaries that prevent buyers from directly contacting sellers.

Various embodiments have been described for issuing electronic seals of certification to online entities, such as online merchants. These and other embodiments are within the scope of the following claims.